CHSH
Cerha Hempel Spiegelfeld Hlawati
Rechtsanwälte GmbH

Universitäten Forschung Datenschutz

„Verwaltung I“ – Dokumentations- und Informationspflichten

Jänner 2018

Dr. Hans Kristoferitsch, LL.M. (Harvard)

Überblick

I. Dokumentationspflichten

1. Datenverzeichnis nach Art 30 DSGVO
2. Folgenabschätzung
3. Datenschutzbeauftragter
4. Zertifizierung und Nachweisbarkeit

II. Informationspflichten

1. Informationspflichten nach Art 13, 14 DSGVO
2. Betroffenenrechte, insbesondere Auskunftsrecht
3. Data Breach Notification nach Art 33, 34 DSGVO

I. Dokumentationspflichten

1. Das Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO

1.1. Aufzeichnungspflichten

- **Daten-Verzeichnis**
  - Zu erfassen sind sämtliche **Verarbeitungstätigkeiten**
  - Pflicht trifft **Auftraggeber** und nunmehr auch **Dienstleister**
  - **Ausnahme: KMU** (= Unternehmen mit weniger als 250 Mitarbeitern), **es sei denn** die Datenverarbeitungsvorgänge
    - sind mit einem hohen Risiko verbunden; oder
    - erfolgen regelmäßig; oder
    - erfassen sensible oder strafrechtlich relevante Daten
  - Das Verzeichnis muss der Behörde auf Anfrage zur Verfügung gestellt werden

1.2. Allgemeines

- **Form:**
  - Schriftlich zu führen (z.B. Excel)
  - Elektronisches Format auch zulässig → Datenbank
    - Verknüpfung möglich (z.B. Synchronisierung bei Auftragsverarbeitung im Konzern)
    - Möglichkeit verschiedener Ansichten → Auszug für Behörde kann auf die gesetzlich vorgeschriebenen Informationen beschränkt werden
    - Ermöglicht Analysen und gezielte Suchen (z.B. bei der Bearbeitung von Betroffenen-Anfragen)

- **„Lebendes Verzeichnis“**
  - Regelmäßig zu aktualisieren
  - Dezentrale Bearbeitung empfehlenswert

1.3. Inhalt des Verzeichnisses (1)

- **Zu erfassen sind im Verzeichnis des Verantwortlichen:**
  - Name und Kontaktdaten des Verantwortlichen & Datenschutzbeauftragten
  - Zwecke der Verarbeitung
  - Fristen für Löschung
  - Übermittlungen,
  - Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
  - Kategorien von Empfängern (ggf Übermittlungen von personenbezogenen Daten an ein Drittland)
  - technische und organisatorische Datenschutz-Maßnahmen

1.3. Inhalt des Verzeichnisses (2)

- **Zu erfassen sind im Verzeichnis des Auftragsverarbeiters:**
  - Name und Kontaktdaten des Auftragsverarbeiters & Datenschutzbeauftragten
  - Kategorien von Verarbeitungen
  - gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland
  - technische und organisatorische Datenschutz-Maßnahmen

1.4. Beispiel

I.	Name und Zweck der Verarbeitungstätigkeit	System	Nummer der Verarbeitungstätigkeit
xxxx		xxxx	xxxx

II.	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	
No.	Kategorien betroffener Personen / Kategorien personenbezogener Daten	vorgesehene Frist für die Löschung
1.	**xxxx [Kategorie von Betroffenen 1]**	
1.1	xxxx [Datenart 1]	
1.2	xxxx [Datenart 2]	
1.3		
1.4		
1.5		
2.	**xxxx [Kategorie von Betroffenen 2]**	
2.1	xxxx [Datenart 1]	
2.2	xxxx [Datenart 2]	
2.3		
2.4		
2.5		

III.	Auftragsdatenverarbeiter				
No.	Name	Addresse und Kontaktdaten	Titel und Datum des Dienstleistervertrags	Falls der Auftragsdatenverarbeiter außerhalb des EWR	
				Land	Rechtsgrundlage
1.					
2.					
3.					
4.					
5.					

IV.	Übermittlung an andere Verantwortliche		
No.	Empfänger oder Kategorie von Empfängern	Falls der andere Verantwortliche außerhalb des EWR	
		Land	Rechtsgrundlage
2.			
3.			
4.			
5.			

V.	Beschreibung spezieller Datensicherheitsmaßnahmen	

Name der Datenanwendung; Beschreibung des Zwecks (Wie und wozu werden die Daten verarbeitet?)

Individuelle Nummer für jede Datenanwendung zur klaren Identifikation

I.	Name und Zweck der Verarbeitungstätigkeit	System	Nummer der Verarbeitungstätigkeit
	Geschäftskorrespondenz	Outlook	ABC_1

Bezeichnung der Software

II.	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	
No.	Kategorien betroffener Personen / Kategorien personenbezogener Daten	vorgesehene Frist für die Löschung
1.	**Kunden**	
1.1	Absender	**7 Jahre**
1.2	Empfänger	
1.3	Uhrzeit Empfang / Versand	
	etc	
2.	**Mitarbeiter**	
1.1	Absender	**7 Jahre**
1.2	Empfänger	
1.3	Uhrzeit Empfang / Versand	
	etc	

Kategorien betroffener Personen und Datenkategorien, z.B. Kunden (oder bei juristischen Personen: Ansprech-partner beim Kunden)

Löschfristen (möglichst konkret, z.B. monatlich)

Auftragsverarbeiter inkl Anschrift und Details zum Vertrag (könnte im Dokument hinterlegt werden)

III.	Auftragsdatenverarbeiter				
No.	Name	Addresse und Kontaktdaten	Titel und Datum des Dienstleistervertrags	Falls der Auftragsdatenverarbeiter außerhalb des EWR	
				Land	Rechtsgrundlage
1.	Backup Provider	Main Street 1,New York City, New York 10024, USA	Processing Agreement (01.01.2017)	USA	Standardvertragsklausein
2.	Schwestergesellschaft A	Direkt Nebenan 1, 1010 Wien	Service-Vertrag (01.05.2016)		
3.					
4.					
5.					

Interne und externe Auftragsverarbeiter

Wenn der Auftragsverarbeiter außerhalb des **EWR** sitzt: Angabe der Rechtsgrundlage für die Übermittlung ins Drittland

Empfänger der Daten, die keine Auftragsverarbeiter sind (auch konzernintern!)

IV.	Übermittlung an andere Verantwortliche		
No.	Empfänger oder Kategorie von Empfängern	Falls der andere Verantwortliche außerhalb des EWR	
		Land	Rechtsgrundlage
1.	Banken zur Abwicklung des Zahlungsverkehrs		
2.	Rechtsvertreter im Geschäftsfall	China	Standardvertragsklauseln
3.	Wirtschaftstreuhänder für Zwecke des Auditing		

Gegebenenfalls wieder Angaben zur Übermittlung ins Drittland

Beschreibung der ergriffenen technischen und organisatorischen Maßnahmen („TOMs“) zur Sicherstellung der Datensicherheit

V.	Beschreibung spezieller Datensicherheitsmaßnahmen	
1.	Zutrittsbeschränkung	Der Zutritt zu den Räumen, in denen sich die Rechner befinden ist nur den hierzu berechtigten Mitarbeitern gestattet. Besucher werden in Besucherlogbüchern erfasst, etc.
2.	Zugriffsbeschränkung	Es wurde ein Zugriffsberechtigungssystem mit Passwortschutz implementiert. Die Passwörter sind alle sechs Wochen zu wechseln und müssen mindestens 8 Zeichen enthalten. Die Zugriffstabellen werden von Max Mustermann verwaltet.

Kategorisierung zB nach Zutrittsbeschränkungen, Zugriffsbeschränkungen, Betriebsbeschränkung, Protokollierungspflicht, Dokumentationspflichten

2. Folgenabschätzung

2. Folgenabschätzung (1)

- **Verstärkte Datenschutzautonomie der Auftraggeber**
  - **Bisher:** Meldung beim DVR oder Genehmigung durch Datenschutzbehörde
  - **Künftig:**
    - Folgenabschätzung durch Auftraggeber *vor* der Datenverarbeitung, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht
    - Konsultation mit Behörde bei tatsächlich bestehender datenschutzrechtlicher Risikosituation
    - Behörde kann Empfehlung aussprechen und gegebenenfalls auch die Verarbeitung untersagen

2. Folgenabschätzung (2)

- Art 35 (3): Eine Folgenabschätzung ist insbesondere in folgenden Fällen durchzuführen:
  - Automatische und umfassende Bewertung **persönlicher Aspekte** natürlicher Personen gestützt auf automatisierte Verarbeitung / Profiling als Grundlage für wesentliche Entscheidungen,
  - Umfangreiche Verarbeitung **besonderer Kategorien** von Daten einschließlich strafrechtlich relevanten Daten,
  - Systematische, umfangreiche **Überwachung** öffentlich zugänglicher Bereiche.

2. Folgenabschätzung (3)

- Art 35 (7) DSGVO: Die Folgenabschätzung enthält zumindest
  - Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck
  - Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen
  - Zur Bewältigung der Risiken geplante Abhilfemaßnahmen […] durch die der Schutz personenbezogene Daten sichergestellt und der Nachweis dafür erbracht wird, dass DSGVO eingehalten wird […]

2. Folgenabschätzung (4)

- Art 35 (4): Aufsichtsbehörde erstellt **Liste** von Verarbeitungsvorgängen, für die Folgenabschätzung zu erstellen ist.
- Art 35 (5): Aufsichtsbehörde kann **Liste** von Verarbeitungsarten erstellen, für die keine Folgenabschätzung erforderlich ist.
- **Guidelines** der EU Datenschutzbehörden zu Folgenabschätzung noch ausständig.

3. Datenschutzbeauftragter

- Bestellung eines Datenschutzbeauftragten nur in bestimmten Fällen verpflichtend
- **Aufgaben:**
  - Beratung des Auftraggebers und dessen Mitarbeiter in datenschutzrechtlichen Angelegenheiten
  - Überwachung der datenschutzrechtlichen Compliance
  - Stellungnahmen im Rahmen der Folgenabschätzungen
  - Kontaktperson für die Datenschutzbehörde
- Nehmen eine **besondere Stellung** im Unternehmen ein
- Datenschutzbeauftragte sind zur Geheimhaltung verpflichtet
- Für eine Unternehmensgruppe bzw mehrere Behörden kann ein gemeinsamer Datenschutzbeauftragten bestellt werden

4. Zertifizierung und Nachweisbarkeit

- Datenschutz-Aufsichtsbehörden können
  - Zertifizierungsstellen akkreditieren und
  - Zertifizierungskriterien festlegen.
- Zertifizierungen als **Nachweis** für die Einhaltung
  - der Anforderungen des Privacy by Design / Default,
  - der Anforderungen an die Datensicherheit,
  - eines angemessenen Datenschutzniveaus bei Datenexport in Drittstaaten
- **Guidelines** der EU Datenschutzbehörden zu Zertifizierung sind für 2017 angekündigt

II. Informationspflichten

1. Informationspflichten nach Art 13, 14 DSGVO

1.1. Allgemein (1)

- Betroffene sind darüber zu informieren,
  - **von wem**,
  - auf welcher **Rechtsgrundlage**,
  - und zu welchem **Zweck** ihre Daten verarbeitet und
  - **an wen** sie übermittelt werden
- Grundlegende Voraussetzung für die Ausübung der Betroffenenrechte
- Schaffung der hierfür erforderlichen **Transparenz**, vgl Art 5 Abs 1 lit a DSGVO bzw Art 8 Abs 2 S 1 GRCh

1.1. Allgemein (2)

- Unterschiedliche Informationspflichten je nach Art der Erhebung (Direkterhebung vs sonstige Art der Erhebung)
- **Direkterhebung:** jede Erhebung personenbezogener Daten mit Kenntnis und unter Mitwirkung der betroffenen Person
- Form der Information: **geeignete Maßnahmen**, vgl Art 12 Abs 1
  - Präzision, Transparenz, Verständlichkeit, leichte Zugänglichkeit, klare und einfache Sprache
  - Websites / Druckwerke
  - Intranet vs Anhang zum Arbeitsvertrag bei Verarbeitung im Beschäftigungskontext
- Sanktionen bei Verstoß: **Geldbußen**, vgl Art 83 Abs 5 lit b
- Behördlicher und gerichtlicher Rechtsschutz

1.2. Art 13 DSGVO

- Direkterhebung:

  Informationspflicht bei Erhebung von personenbezogenen Daten **bei der betroffenen Person**
- Erhebung von Daten mit Doppelbezug: keine Information Dritter erforderlich
- Erneute Informationspflicht bei **nachträglicher Zweckänderung** der Verarbeitung, Art 13 Abs 3
- **Keine** Informationspflicht, wenn die Betroffenen bereits über diese Informationen verfügen, vgl Art 13 Abs 4.

1.3. Art 14 DSGVO (1)

- außerhalb der Direkterhebung

  Informationspflicht, wenn die personenbezogenen Daten **nicht bei der betroffenen Person erhoben** wurden
- Entspricht weitestgehend dem Art 13
- **Nachgelagertes Informationsverhalten**, daher spezifische Fristenregelung in Art 14 Abs 3:
  - unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer **angemessenen Frist nach Erlangung** der personenbezogenen Daten, **längstens jedoch innerhalb eines Monats**,
  - falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, **spätestens zum Zeitpunkt der ersten Mitteilung** an sie, oder,
  - falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, **spätestens zum Zeitpunkt der ersten Offenlegung**.

1.3. Art 14 DSGVO (2)

- **Keine** Informationspflicht, wenn
  - die Betroffenen über die Informationen bereits verfügen,
  - die Erteilung der Information unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist,
  - die Verarbeitung gesetzlich vorgesehen ist oder
  - die Daten dem Berufsgeheimnis unterliegen, Art 14 Abs 5

2. Betroffenenrechte, insbesondere Auskunftsrecht

2.1. Überblick

- Auskunft zu den über ihre Person gespeicherten Daten
- Einschränkung / Löschung über ihre Person gespeicherten Daten, bei Vorliegen der Voraussetzungen hierfür (z.B. für Zweckerreichung nicht mehr notwendig, Widerruf einer Einwilligung)
- Richtigstellung der über ihre Person (falsch) gespeicherten Daten
- Data Breach Notification

2.2. Verlangen

- Formfrei / kein Formzwang
- Identität des Betroffenen muss nicht aktiv nachgewiesen werden
- Bei berechtigten Zweifeln an der Identität des Betroffenen kann der Verantwortliche zusätzliche Informationen anfordern (z.B. Ausweiskopie)
- Berechtigte Zweifel z.B. bei Telefonanrufen oder bei Verwendung von Fantasie-E-Mail-Adressen (prinzessin333@hotmail.com)

2.3. Weigerung

- Bei Verweigerung: dennoch Verständigung des Betroffenen innerhalb der Frist unter Angabe der Gründe und Information über die Möglichkeit einer Beschwerde bei der Datenschutzbehörde
- Mögliche Gründe:
  - Gesetzliche Beschränkungen stehen dem Auskunftsrecht entgegen
  - Auskunftsverlangen ist offenkundig unbegründet oder wegen Häufigkeit exzessiv

2.4. Kosten und Frist

Kosten

- Grundsätzlich kein Anspruch auf Kostenersatz
- bei Verlangen auf Übermittlung mehrerer Kopien kann jedoch ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangt werden
- bei offenkundig unbegründeten oder exzessiven Anträgen eines Betroffenen kann ebenfalls ein angemessenes Entgelt verlangt werden

Frist

- 1 Monat (ausnahmsweise: 2 Monate + Verständigung des Betroffenen innerhalb der Monatsfrist inkl. Angabe der Gründe) müssen eingehalten werden

2.5. Recht auf Auskunft (1)

- Auf Verlangen des Betroffenen hat Verantwortlicher Auskunft zu erteilen
- Pflichten des Verantwortlichen:
  - Mitteilung, **ob** personenbezogene Daten des Betroffenen verarbeitet werden
  - Wenn ja, dann Pflicht zur **Auskunft** über diese Daten
  - Zurverfügungstellung einer **Kopie** der personenbezogenen Daten, die Gegenstand der Verarbeitung sind

2.5. Recht auf Auskunft (2)

- **Negativauskunft**, wenn keine Daten des Betroffenen verarbeitet werden
- **Inhalt** der Auskunft, wenn eine Verarbeitung erfolgt:
  - Verarbeitungszweck
  - Kategorien der personenbezogenen Daten
  - Empfänger oder Kategorien von Empfängern
  - Falls möglich: geplante Dauer der Speicherung
  - Information über das Bestehen des Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder über das Widerspruchsrecht
  - Information über das Bestehen des Beschwerderechts bei der Datenschutzbehörde
  - Gegebenenfalls Information über die Herkunft der Daten
  - Information über automatisierte Entscheidungsfindungssysteme („Profiling“)
  - Bei internationalen Datentransfers, Information über geeignete Garantien

3. Data Breach Notification, Art 33, 34 DSGVO

- Verletzung des Schutzes personenbezogener Daten (= Verlust der vollständigen Kontrolle über die Daten, z.B. „Hackerangriffe“, „Trojaner“)
- Information der **Betroffenen**
- NEU: Verständigung der zuständigen **Datenschutzbehörde** binnen 72 Stunden nach Bekanntwerden der Verletzung
- **Vorbeugen:** Data Breaches durch Definition, Umsetzung und regelmäßige Überprüfung von Sicherheitsmaßnahmen für die interne IT sowie Dienstleister bestmöglich vermeiden – vgl. auch Art 25, 30 DSGVO: Privacy by Design / Default

CHSH
Cerha Hempel Spiegelfeld Hlawati
Rechtsanwälte GmbH

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Hans Kristoferitsch, LL.M.
+43 / 1 / 514 35 – 291
hans.kristoferitsch@chsh.com